62-45

ON THE APPLICABILITY OF BINARY CORRECTING CODES IN TRANSMISSION CHANNELS OF DISCRETE INFORMATION

By

L. M. Fink

UNEDITED ROUGH DRAFT TRANSLATION

ON THE APPLICABILITY OF BINARY CORRECTING CODES IN TRANSMISSION CHANNELS OF DISCRETE INFORMATION*

By L. M. Fink

English Pages: 13

Source: Radiotekhnika, Vol. 16, No. 10, 1961, PP 3-9

ASTAR 2539
SC-990
SOV/108-61-16-10

ON THE APPLICABILITY OF BINARY CORRECTING CODES IN TRANSMISSION CHANNELS OF DISCRETE INFORMATION*

L. M. Fink

Using asymptotic expressions for the equivalent probability of error, the conditions of "acceptability" are derived for a correcting code. These conditions are satisfied by very few of the codes described in the literature. In channels with fading, these conditions may be made less rigid if the measure and decorrelation of error are taken in constructing the code.

1. In order to evaluate correcting codes it is convenient to use the notion of "equivalent probability of error" [1]. Let the probability of incorrect reception of a symbol in a binary symmetric channel equal p. Using a correcting code in this channel, it is possible to send a sequence of n symbols with a probability of correct decoding Q(n). The quantity of information contained in this sequence is k binary units, where $k \leq n$. The value

$$R = \lim_{n \to \infty} \frac{n - \kappa}{n} \qquad (1)$$

* Reported in June, 1961, at the All-Union Scientific Session of the A. S. Popov Scientific and Technical Society of Radio and Electronics.

will be, as usual, called the redundance of the code.

This same quantity of information could be sent with the same reliability without using a correcting code in a binary symmetric channel if the probability of correct reception of the symbol were equal to $[Q(n)]^{1/k}$. With an increase in n this probability converges on a limit which we shall call the equivalent probability of correct reception of a symbol. Its complement with respect to unity

$$p_e = 1 - \lim_{n\to\infty}[Q(n)]^{1/k} = 1 - \lim_{n\to\infty}[Q(n)]^{\frac{1}{n(1-R)}} \qquad (2)$$

we shall call the equivalent probability of error.

For group (systematic) codes and also for any correcting codes in which closed code combinations of a definite length are used, one may dispense with the limit transformation in expressions, having taken as the valu n the number of symbols in the code combination. In this, if $p \ll 1$, the equivalent probability of error for all practical purposes coincides with the "specific probability of error," introduced by V. I. Siforov [2].

The correcting properties of a code are based on the fact that at least in some range of values of p the inequality holds

$$p_e < p, \qquad (3)$$

wherein the ratio $\frac{p_e}{p}$ usually decreases with an increase in p. However, as has already been repeatedly mentioned, Inequality (3) is not always sufficient to justify the use of a correcting code in a given channel. In most actual channels the magnitude of p is a function of the duration of a symbol τ. Therefore, the magnitude of p should be made comparable not with the probability of incorrect reception of a symbol of a correcting code $p = p(\tau)$, but with that probability of error p' which would hold if binary symbols were

transmitted in an actual channel at the same rate at which information is transmitted using a correcting code.

Obviously,

$$p' = p\left(\tau\frac{n}{\kappa}\right) = p\left(\frac{\tau}{1-R}\right). \tag{4}$$

Only when the inequality

$$p_e < p' \tag{5}$$

is fulfilled, if only for all $p' < p_0$, where p_0 is a given number, may one speak about the advantage of using a correcting code. In the opposite case, it would be safer to send information at the same rate using a code without redundancy.

Let us consider these codes satisfying Condition (5) at values of p' less than some p_0 as applicable for a given code. The problem of the practical advantage of using a code is a function also of many other conditions, in particular of the complexity and reliability of the coding and decoding apparatus, on the value p_0, of what degree Inequality (5) is fulfilled, etc.

2. For Hemming's codes* which correct m errors in a combination of n symbols, Q(n) is expressed simply:

$$Q(n) = \sum_{i=0}^{m} C_n^i p^i (1-p)^{n-i} = 1 - \sum_{i=m+1}^{n} C_n^i p^i (1-p)^{n-i}. \tag{6}$$

If $p \ll 1$, in the latter summation only the first term may be taken into account and the equivalent probability of error may be expressed asymptotically in the form

* By Hemming's codes are meant systematic codes in which all errors of multiple m are corrected and errors of a higher multiple are not corrected.

$$p_e \sim \frac{1}{\kappa} C_n^{m+1} p^{m+1}. \qquad (7)$$

Analogously, for group codes[3]

$$Q(n) = \sum_{i=0}^{n} \alpha_i p^i (1-p)^{n-i}, \qquad (6')$$

where α_i is the quantity of i-th correctable errors. At sufficiently low values of p,

$$p_e \sim \frac{1}{\kappa} (C_n^{m+1} - \alpha_{m+1}) p^{m+1}, \qquad (7')$$

where m is the highest multiple of fully correctable errors (i.e., at $i \leq m$, $\alpha_i = C_n^i$). Apparently, for any correcting code these constants a and m may be determined so,

$$\lim_{p \to 0} \frac{p_e}{a p^{m+1}} = 1. \qquad (8)$$

3. Let the channel in question be stationary and only additive interference in the form of normal white noise act in it. Then, as is known, using the optimal element coherent reception, one may ensure the minimal probability of error

$$p = \frac{1}{2} [1 - \Phi(h)], \qquad (9)$$

where h is a value proportional to the square root of the energy of the signal element used for transmission of one symbol (the accurate expression for h is a function of the transmission method and is of no further interest),

$$\Phi(h) = \sqrt{\frac{2}{\pi}} \int_0^h \exp\left(-\frac{x^2}{2}\right) dx.$$

Using the asymptotic expression for Φ, we obtain the dependence

$$\lim_{h\to\infty} \frac{p}{\frac{1}{\sqrt{2\pi}h}\exp\left(-\frac{h^2}{2}\right)} = 1. \tag{10}$$

A similar dependence may be written for p', taking Expression (4) into account. Since the energy of the signal element is proportional to τ, then, preserving the symbol $\underline{h}$ when a correcting code is used, we find that at an increased τ by a factor of $\frac{1}{1-R}$ the corresponding parameter takes the value

$$h' = \frac{h}{\sqrt{1-R}}. \tag{11}$$

Hence

$$\lim_{h\to\infty} \frac{p'}{\frac{\sqrt{1-R}}{\sqrt{2\pi}h}\exp\left[-\frac{h^2}{2(1-R)}\right]} = 1. \tag{12}$$

On the other hand, from (8) and (10)

$$\lim_{h\to\infty} \frac{P_e}{\frac{a}{(\sqrt{2\pi})^{m+1}h^{m+1}}\exp\left[-\frac{(m+1)h^2}{2}\right]} = 1. \tag{13}$$

Comparing (12) and (13), we have

$$\lim_{h\to\infty}\frac{p_e}{p'} = \lim_{h\to\infty}\frac{a}{\sqrt{1-R}(\sqrt{2\pi})^m h^m}\exp\left[\left(\frac{1}{1-R}-m-1\right)\frac{h^2}{2}\right]. \tag{14}$$

If $\frac{1}{1-R} > m+1$, the right-hand member of (14) will increase without limit and, therefore, Condition (5) will not be fulfilled. If, conversely, $\frac{1}{1-R} \leq m+1$, the limit of the right-hand member will equal zero; therefore, at sufficiently high values of $\underline{h}$ Inequality (5) will be fulfilled.

Thus, for a stationary channel with additive interference in the form of white noise, the condition of applicability of a correcting code is

$$m \geq \frac{R}{1-R} \tag{15}$$

For group codes this condition may be written in the form

$$m \geq \frac{n}{k} - 1 \qquad (15')$$

4. It is interesting to note that when incoherent reception is used in a stationary channel with additive normal noise, the condition of applicability of a correcting code (15) is almost unchanged.

Let us limit ourselves to the case when an orthogonal system is used with an active pause [4]. The probability of error in this equals

$$p = \frac{1}{2} \exp\left(-\frac{h^2}{2}\right) \qquad (16)$$

Taking (11) and (8) into account, we find

$$p' = \frac{1}{2} \exp\left[-\frac{h^2}{2(1-R)}\right] = \frac{1}{2}(2p)^{\frac{1}{1-R}}, \qquad (17)$$

$$\lim_{h\to\infty} \frac{p_e}{\frac{a}{2^{m+1}} \exp\left(-\frac{m+1}{2} h^2\right)} = 1 \qquad (18)$$

and, therefore,

$$\lim_{h\to\infty} \frac{p_e}{p} = \lim_{h\to\infty} \frac{a}{2^m} \exp\left[\left(\frac{1}{1-R} - m - 1\right)\frac{h^2}{2}\right]. \qquad (19)$$

Hence, it is apparent that condition of applicability of a correcting code is

$$m > \frac{R}{1 - R} \qquad (20)$$

or for group codes,

$$m > \frac{n}{k} - 1. \qquad (20')$$

Although the equation $m = \frac{R}{1 - R}$ in (15) formally satisfies the requirement of applicability, in most cases the equation corresponds

to codes whose use is, in practice, unadvantageous. In these cases the difference between p_e and p' is usually found to be very insignificant and manifests itself only when the magnitude of p' is so small that any complication in the apparatus so that $p_e < p'$ does not give real advantages. Thereofre, for stationary channels with additive white noise, in coherent as well as incoherent reception, only those codes for which the inequality $m > \frac{R}{1 - R}$ is fulfilled are of practical interest.

5. At first glance it can be shown that the simplest way of fulfilling condition (20) is to choose a code with lowest possible redundancy which will correct even individual errors ($m = 1$, $R < 0.5$). However, this solution is often found to be unsuccessful. When redundancy is low, a correcting code does not correct errors if the initial probability of error is not very low. As an example let us examine the optimal group codes in the work of D. Slepian [3]. The data on these is given in Table 1.

The applicable codes are denoted by asterisks. Thus, of the 42 group codes examined, only eight are applicable.

In order to evaluate the effectiveness of an applicable correcting code the boundary probability of error p_0 and the relationship between $\underline{m}$ and R are of essential value. Limiting ourselves to the case of incoherent reception, from (16), (17), and (19) we can obtain the asymptotic expression

$$\ln \frac{p_e}{p} \sim \ln \frac{a}{2^m} + (m - R - Rm) \ln(2p'), \qquad (21)$$

which is the equation of an asymptotic straight line for the dependence between $\ln \frac{p_e}{p'}$ and $\ln p'$. Figure 1 shows this dependence for four groups calculated by the accurate formulas (2) and (17). In the

of group codes (5.2), (11.4) etc., the first number represents $\underline{n}$ and the second $\underline{k}$. Code (5.2) is not applicable, therefore, for it $p_e > p'$ always. The remaining three codes are applicable, however, code (7.4) and especially (11.4) are not suitable in practice owing to the very low value of p_o and the small difference between p_e and p'. As is apparent from Fig. 1, in the range of not very high values of p', an asymptotic straight line is a sufficiently good approximation of this dependence. Therefore, the approximate value of the boundary probability of error p_o may be obtained from (21), having made $p_e = p' = p_o$,

$$\ln p_o \approx \frac{1}{m - R - Rm} \ln \frac{2^m}{a} - \ln 2. \qquad (22)$$

TABLE 1

n	κ	m	a	R	$\frac{n}{\kappa}-1$	n	κ	m	a	R	$\frac{n}{\kappa}-1$
3	1	1	3	0,67	2	6	2	1	3	0,67	2
4	2	0	1	0,5	1	6	3	1	5,3	0,5	1
5	2	1	4	0,6	1,5	6	4	0	0,75	0,67	2
5	3	0	0,67	0,4	0,67	7	2	1	1,5	0,71	2,5
7	3	1	2,67	0,57	1,33	10	4	1	1,5	0,6	1,5
7	4	1	5,25	0,43	0,75*	10	5	1	4,8	0,5	1
7	5	0	0,8	0,29	0,4	10	6	1	6,67	0,4	0,67*
8	2	2	14,5	0,75	3	10	7	0	0,43	0,3	0,43
8	3	1	2,67	0,685	1,67	10	8	0	0,87	0,2	0,25
8	4	1	5,25	0,5	1	11	2	3	52	0,82	4,5
8	5	0	0,2	0,375	0,6	11	3	2	13	0,73	2,67
8	6	0	0 83	0,25	0,33	11	4	2	26	0,64	1,75*
9	2	2	10	0,78	3,5	11	6	1	5,83	0,45	0,83*
9	3	1	1	0,67	2	11	7	1	7,29	0,36	0,57*
9	4	1	2,75	0,56	1,25	11	8	0	0,5	0,27	0,375
9	5	1	6	0,44	0,8*	11	9	0	0,9	0,18	0,22
9	6	0	0,33	0,33	0,5	12	2	3	35	0,83	5
9	7	0	0,85	0,22	0,29	12	3	2	6,67	0,75	3
10	2	2	5	0,8	4	12	7	1	6,71	0,42	0,71*
10	3	2	18,7	0,7	2,33	12	8	1	7,87	0,33	0,5 *
						12	9	0	0,56	0,25	0,33

The second value describes the degree of suitability of a code

and is the slope of the straight line (21), which may be called the "effectiveness" of the code

$$E = m - R - Rm, \tag{23}$$

or for group codes

$$E = \frac{k}{n}(m + 1) - 1. \tag{23'}$$

For inapplicable codes $E \leq 0$, which coincides with condition (20). For applicable codes, the larger E, the more rapidly the gain from using the code at decreased p' grows. Table 2 shows the calculated values of E, and also the approximate values of p_0, for the eight applicable group codes.

TABLE 2

n	κ	m	a	E	p_0
7	4	1	5,25	1/7	$\approx 1\cdot10^{-3}$
9	5	1	6	1/9	$\approx 4\cdot10^{-5}$
10	6	1	6,67	1/5	$\approx 1\cdot10^{-3}$
11	4	2	26	1/11	$\approx 1\cdot10^{-9}$
11	6	1	5,83	1/11	$\approx 5\cdot10^{-5}$
11	7	1	7,29	3/11	$\approx 6\cdot10^{-3}$
12	7	1	6,71	1/6	$\approx 3\cdot10^{-4}$
12	8	1	7,87	1/3	$\approx 5\cdot10^{-3}$

Code (12.8) has the highest effectiveness. Code (11.7) has almost the same effectiveness and the highest value of p_0. Only these two codes of all those examined can provide any noticeable advantage in a stationary channel with additive noise at sufficiently high signal-to-noise ratio, satisfying the condition $p' < p_0$. For a more substantial increase in noise stability when using a group

code, it is necessary, apparently to use longer code combinations at higher values of m

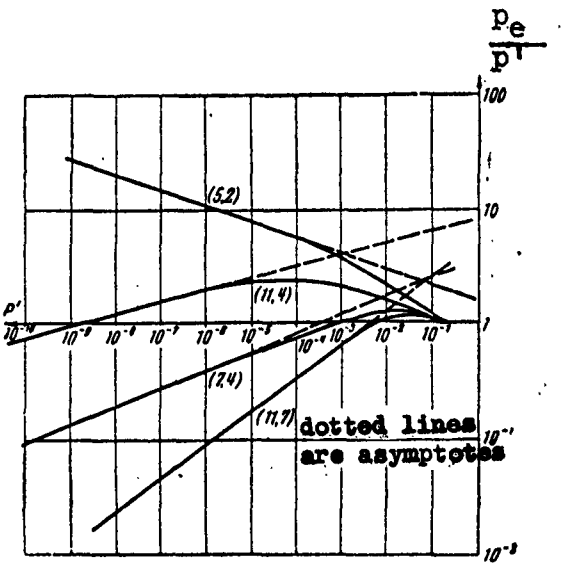

Fig. 1.

6. As is known, due to fading many radio channels are not stationary. In most cases the relationships between the duration of a symbol, the length of a code combination and the fading-correlation time are such that for the reception time of one code combination the channel may be considered stationary, i.e., the value of p for this time is almost unchanged. Under these conditions, all these conclusions become correct during fading also. It is only necessary to take into account the slow changes of p, as a result of which some code combinations are received with a probability of error which is substantially greater than its mean value. This imposes even more rigid requirements upon the boundary value p_o. If the code is theoretically applicable, but the value of p_o does not exceed by much the mean probability of error in an actual channel, then a significant number of code combinations will be received at $p' > p_o$ and the use of the code will yield no gain, but will decrease noise stability.

The matter is entirely different when the measures of "error randomization" are used in constructing the code. This is accomplished by separating in time the transmission of symbols which are incorporated in a single combination of the correcting code [1 and 5]. When the spacing is sufficient, errors in the reception of various symbols may be considered independent. As is known [6] in this the probability of error (in the case of Rayleigh fading) is

$$p = \frac{1}{h^2 + 2} . \tag{24}$$

Taking (4) and (8) into account, we have

$$\lim_{h\to\infty} \frac{p_e}{p^r} = \lim_{h\to\infty} \frac{a}{1-R} h^{-2m} . \tag{25}$$

Thus, at any $m \geq 1$ and at sufficiently high values of h, condition (5) is fulfilled and the code is applicable for a channel with fading during error randomization. In particular, any group code (transformed for error randomization) is applicable if it permits correction of all individual errors in the code combination; therefore, any Hemming code is applicable.

In practice, complete error randomization is difficult to attain. Therefore, it is advantageous to use those codes which are applicable without randomization. Even if randomization is found to be incomplete, the use of the correcting code will not lead to poorer reception.

The most simple error randomization is attained by using not the group, but the so-called iterated [7] or recurrent [8] codes. The question of the applicability of iterated codes, and also codes with correct error "splashes," will be examined in another article.

Submitted November 4, 1960

REFERENCES

1. L. M. Fink, Elementy Teorii Radiotelegrafnoy Svyazi, Dissertatsiya VKAS, 1958.

2. V. I. Siforov, "Elektrosvyaz'," No. 1, 1957.

3. D. Slepian, BSTJ, Vol. 35, No. 1, 1956.

4. L. M. Fink, "Radiotekhnika," Vol. 14, No. 1, 1959.

5. A. A. Kharkevich and E. L. Blokh, "Elektrosvyaz'," No. 4, 1960.

6. L. M. Fink, "Radiotekhnika," Vol. 14, No. 9, 1959.

7. L. M. Fink and V. I. Shlyapoberskiy, Avtorskoye Svidetel'stvo No. 17748 s Priortetom ot 14 Feb. 1955.

8. D. W. Hagelbarger, BSTJ, Vol. 38, No. 4, 1959.

DISTRIBUTION LIST

DEPARTMENT OF DEFENSE	Nr. Copies
HEADQUARTERS USAF	
AFCIN-3D2	1
OTHER AGENCIES	
CIA	1
NSA	2
AID	2
OTS	2
AEC	2
PWS	1
PGE	1

MAJOR AIR COMMANDS	Nr. Copies
AFSC	
SCFTR	1
ARO	1
ASTIA	10
TD-Bla	3
RADC (RAY)	1
SSD (SSF)	1
ASD (DCF)	1
ESD (ESY)	1
AFSWC (SWY)	1
AFMTC (MTW)	1
APGC (PGF)	1